

(19) World Intellectual Property Organization  
International Bureau



(43) International Publication Date  
8 March 2001 (08.03.2001)

PCT

(10) International Publication Number  
**WO 01/17251 A1**

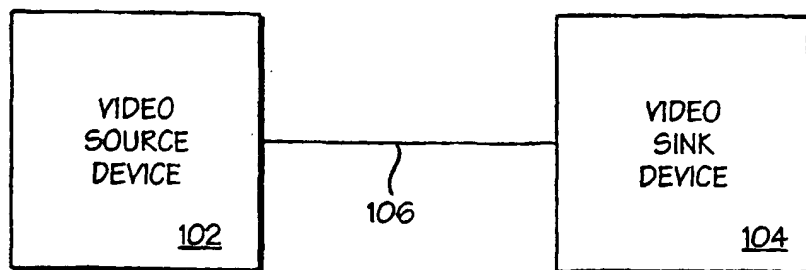
- (51) International Patent Classification<sup>7</sup>: H04N 7/167 (74) Agents: MALLIE, Michael, J. et al.; Blakely, Sokoloff, Taylor & Zafman LLP, 7th floor, 12400 Wilshire Boulevard, Los Angeles, CA 90025 (US).
- (21) International Application Number: PCT/US00/22785
- (22) International Filing Date: 17 August 2000 (17.08.2000) (81) Designated States (*national*): AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CR, CU, CZ, DE, DK, DM, DZ, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, TZ, UA, UG, US, UZ, VN, YU, ZA, ZW.
- (25) Filing Language: English
- (26) Publication Language: English
- (30) Priority Data:  
09/385,592 29 August 1999 (29.08.1999) US (84) Designated States (*regional*): ARIPO patent (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GW, ML, MR, NE, SN, TD, TG).
- (71) Applicant (*for all designated States except US*): INTEL CORPORATION [US/US]; 2200 Mission College Boulevard, Santa Clara, CA 95052 (US).
- (72) Inventors; and
- (75) Inventors/Applicants (*for US only*): GRAUNKE, Gary, L. [US/US]; 362 NE Hillwood Drive, Hillsboro, OR 97124 (US). LEE, David, A. [US/US]; 740 SW Willow Creek Drive, Beaverton, OR 97006 (US). FABER, Robert, W. [US/US]; 942 NE Third Avenue, Hillsboro, OR 97124 (US).

**Published:**

— With international search report.

*For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.*

(54) Title: DIGITAL VIDEO CONTENT TRANSMISSION CIPHERING AND DECIPHERING METHOD AND APPARATUS



(57) Abstract: A video source device generates a session key for each transmission session wherein a multi-frame video content is to be transmitted to a video sink device. The video source device uses the session key to generate a successive number of frame keys. The frame keys in turn are used to generate corresponding pseudo random bit sequences for ciphering the

corresponding frames to protect the video content from unauthorized copying during transmission. The video sink device practices a complementary approach to decipher the received video content. In one embodiment, both devices are each provided with an integrated block/stream cipher to practice the transmission protection method.

Best Available Copy

WO 01/17251 A1

**Digital Video Content Transmission Ciphering And Deciphering**  
**Method And Apparatus**

**BACKGROUND OF THE INVENTION**

1. **Field of the Invention**

The present invention relates to the field of content protection. More specifically, the present invention addresses the provision of protection to digital video content to facilitate their secure transmission from a video source device to a video sink device.

2. **Background Information**

In general, entertainment, education, art, and so forth (hereinafter collectively referred to as "content") packaged in digital form offer higher audio and video quality than their analog counterparts. However, content producers, especially those in the entertainment industry, are still reluctant in totally embracing the digital form. The primary reason being digital contents are particularly vulnerable to pirating. As unlike the analog form, where some amount quality degradation generally occurs with each copying, a pirated copy of digital content is virtually as good as the "gold master". As a result, much efforts have been spent by the industry in developing and adopting techniques to provide protection to the distribution and rendering of digital content.

Historically, the communication interface between a video source device (such as a personal computer) and a video sink device (such as a monitor) is an analog interface. Thus, very little focus has been given to providing protection for the transmission between the source and sink devices. With advances in integrated circuit and other related technologies, a new type of digital interface between video source and sink devices is emerging. The availability of this type of new digital interface presents yet another new challenge to protecting digital

**Figure 5** illustrates the combined block/stream cipher of **Fig. 4** in further detail, in accordance with one embodiment;

**Figure 6** illustrates the block key section of **Fig. 5** in further detail, in accordance with one embodiment;

**Figure 7** illustrates the block data section of **Fig. 5** in further detail, in accordance with one embodiment; and

**Figures 8a-8c** illustrate the stream data section of **Fig. 5** in further detail, in accordance with one embodiment.

### DETAILED DESCRIPTION OF THE INVENTION

In the following description, various aspects of the present invention will be described, and various details will be set forth in order to provide a thorough understanding of the present invention. However, it will be apparent to those skilled in the art that the present invention may be practiced with only some or all aspects of the present invention, and the present invention may be practiced without the specific details. In other instances, well known features are omitted or simplified in order not to obscure the present invention.

Various operations will be described as multiple discrete steps performed in turn in a manner that is most helpful in understanding the present invention. However, the order of description should not be construed as to imply that these operations are necessarily performed in the order they are presented, or even order dependent. Lastly, repeated usage of the phrase "in one embodiment" does not necessarily refer to the same embodiment, although it may.

Referring now to **Figure 1**, wherein a block diagram illustrating an overview of the present invention, in accordance with one embodiment is shown. As illustrated, video source device **102** and video sink device **104** are coupled to each other by digital video link **106**. Video source device **102** provides video content to video sink device **104** through digital video link **106**. In accordance

203). Upon exchanging the above information, source and sink devices 102 and 104 independently generate their respective copies of an authentication key ( $K_m$ ) using  $A_k$  and  $B_k$  (block 204 and 205). For the illustrated embodiment, source device 102 generates its copy of  $K_m$  by summing private keys of its provided array indexed by  $B_k$ , while sink device 104 generates its copy of  $K_m$  by summing private keys of its provided array indexed by  $A_k$ . At this time, if both source and sink devices 102 and 104 are authorized devices, they both possess and share a common secret authentication key  $K_m$ .

In one embodiment, each of source and sink devices 102 and 104 is pre-provided with an array of 40 56-bit private keys by the certification authority.  $A_n$  is a 64-bit random number, and  $K_m$  is 56-bit long. For more information on the above described authentication process, see co-pending U.S. Patent Application, serial number 09/275,722, filed on March 24, 1999, entitled Method and Apparatus for the Generation of Cryptographic Keys, having common inventorship as well as assignee with the present application.

Having authenticated sink device 104, source device 102 ciphers video content into a ciphered form before transmitting the video content to sink device 104. Source device 102 ciphers the video content employing a symmetric ciphering/deciphering process, and using the random number ( $A_n$ ) as well as the independently generated authentication key ( $K_m$ ) (block 206). Upon receipt of the video content in ciphered form, sink device 104 decipheres the ciphered video content employing the same symmetric ciphering/deciphering processing, and using the provided  $A_n$  as well as its independently generated copy of  $K_m$  (block 207).

In accordance with the present invention, as an integral part of ciphering video content, source device 102 derives a set of verification reference values in a predetermined manner (block 208). Likewise, as an integral part of symmetrically deciphering video content sink device 104 also derives a set of verification values in a predetermined manner, and transmits these derived verification values to source device 102 (block 209). Upon receiving each of

Upon generating the session key  $K_s$ , source device 102 generates an initial version of a second random number ( $M_0$ ) (block 304). For the illustrated embodiment, source device 102 first generates a pseudo random bit sequence (at  $p$ -bit per clock) using a stream cipher with the above described random number  $A_n$  and the session key  $K_s$  (in two roles, as another input random number and as the stream cipher key), applying  $C_2$  clocks. Source device 102 derives  $M_0$  from the pseudo random bit sequence, as the bit sequence is generated.

Next, source device 102 generates a frame key ( $K_i$ ) for the next frame (block 306). For the illustrated embodiment,  $K_i$  is generated by block ciphering an immediately preceding version of the second random number  $M_{i-1}$  using the session key  $K_s$  as the block cipher key, and applying  $C_3$  clocks. That is, for the first frame, frame-1, frame key  $K_1$  is generated by block ciphering the above described initial version of the second random number  $M_0$ , using  $K_s$ , and applying  $C_3$  clocks. Additionally, this operation is subsequently repeated at each vertical blanking interval for the then next frame, frame-2, frame-3, and so forth.

Upon generating the frame key  $K_i$ , source device 102 generates the current version of the second random number ( $M_i$ ) (block 302). For the illustrated embodiment, source device 102 first generates a pseudo random bit sequence (at  $p$ -bit per clock) using a stream cipher with the previous version of the second random number  $M_{i-1}$  and the frame key  $K_i$  (in two roles, as another input random number and as the stream cipher key), applying  $C_4$  clocks. Source device 102 derives  $M_i$  from the pseudo random bit sequence, as the bit sequence is generated.

Upon generating the current version of the second random number  $M_i$ , source device 102 again generates a pseudo random bit sequence (at  $p$ -bit per clock) to cipher the frame (block 308). For the illustrated embodiment, source device 102 generates the pseudo random bit sequence using a stream cipher with an immediately preceding version of the second random number  $M_{i-1}$  and frame key  $K_i$  (in two roles, as another input random number and the stream

are 56 clocks in length. Each 64-bit  $M_i$  is formed by concatenating the "lower" 16-bit stream cipher output of each of the last four clocks.

Accordingly, video content may be advantageously transmitted in ciphered form with increased robustness from source device 102 to sink device 104 through link 106 with reduced pirating risk.

**Figure 4** illustrates video source and sink devices of **Fig. 1** in further detail, in accordance with one embodiment. As shown, video source and sink devices 102 and 104 include interfaces 108a and 108b disposed at the respective end of link 106. Each of interfaces 108a and 108b is advantageously provided with cipher 110 of the present invention and XOR 112 to practice the video content protection method of the present invention as described above. Additionally, for ease of explanation, interface 108a is also shown as having been provided with a separate random number generator 114. Except for interfaces 108a and 108b, as stated earlier, video source and sink devices 102 and 104 are otherwise intended to represent a broad category of these devices known in the art.

Random number generator 114 is used to generate the earlier described random number  $A_n$ . Random number generator 114 may be implemented in hardware or software, in any one of a number of techniques known in the art. In alternate embodiments, as those skilled in the art will appreciate from the description to follow, cipher 110 may also be used to generate  $A_n$ , without the employment of a separate random number generator.

Cipher 110 is a novel combined block/stream cipher capable of operating in either a block mode of operation or a stream mode of operation. To practice the video content protection method of the present invention, cipher 110 is used in block mode to generate the above described session key  $K_s$  and frame keys  $K_i$ , and in stream mode to generate the pseudo random bit sequences for the various frames (and indirectly  $M_i$ , as they are derived from the respective bit sequences).

intermediate "keys", which are stored away (in storage locations not shown). The stored intermediate "keys" are then applied to the ciphered text in reversed order, resulting in the deciphering of the ciphered text back into the original plain text. Another approach to deciphering the ciphered text will be described after block key section 502 and data section 504 have been further described in accordance with one embodiment each, referencing Figs. 6-7.

In stream mode, stream key section 506 is provided with a stream cipher key, such as the earlier described session key  $K_s$  or frame key  $K_i$ . Block key section 502 and data section 504 are provided with random numbers, such as the earlier described session/frame keys  $K_s/K_i$  and the derived random numbers  $M_{i-1}$ . "Rekeying enable" signal is set to an "enabled" state, operatively coupling block key section 502 to stream key section 506. Periodically, at predetermined intervals, such as the earlier described horizontal blanking intervals, stream key section 506 is used to generate one or more data bits to dynamically modify the then current state of the random number stored in block data section 502. During each clock cycle, in between the predetermined intervals, both random numbers stored in block key section 502 and data section 504 are transformed. The random number provided to block key section 502 is independently transformed, whereas transformation of the random number provided to data section 504 is dependent on the transformation being performed in block key section 502. Mapping block 506 retrieves a subset each, of the newly transformed states of the two random numbers, and reduces them to generate one bit of the pseudo random bit sequence. Thus, in a desired number of clock cycles, a pseudo random bit sequence of a desired length is generated.

For the illustrated embodiment, by virtue of the employment of the "rekeying enable" signal, stream key section 506 may be left operating even during the block mode, as its outputs are effectively discarded by the "rekeying enable" signal (set in a "disabled" state).

Again, substitution boxes **604** and linear transformation unit **606** may be implemented in a variety of ways in accordance with well known cryptographic principles.

In one implementation for the above described embodiment, each register **602a**, **602b**, **602c**, **702a**, **702b**, **702c** is 28-bit wide. [Whenever registers **602a**-**602c** or **702a**-**702c** collectively initialized with a key value or random number less than 84 bits, the less than 84-bit number is initialized to the lower order bit positions with the higher order bit positions zero filled.] Additionally, each set of substitution boxes **604** or **704** are constituted with seven 4 input by 4 output substitution boxes. Each linear transformation unit **606** or **706** produces 56 output values by combining outputs from eight diffusion networks (each producing seven outputs). More specifically, the operation of substitution boxes **604/704** and linear transformation unit **606/706** are specified by the four tables to follow. For substitution boxes **604/704**, the  $l$ th input to box  $J$  is bit  $l*7+J$  of register **602a/702a**, and output  $l$  of box  $J$  goes to bit  $l*7+j$  of register **602c/702c**. [Bit 0 is the least significant bit.] For each diffusion network (linear transformation unit **606** as well as **706**), the inputs are generally labeled **I0-I6** and the outputs are labeled **O0-O6**. The extra inputs for each diffusion network of the linear transformation unit **706** is labeled **K0-K6**.

	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
SK	8	14	5	9	3	0	12	6	1	11	15	2	4	7	10	13
SK	1	6	4	15	8	3	11	5	10	0	9	12	7	13	14	2
SK	13	11	8	6	7	4	2	15	1	12	14	0	10	3	9	5
SK	0	14	11	7	12	3	2	13	15	4	8	1	9	10	5	6
SK	12	7	15	8	11	14	1	4	6	10	3	5	0	9	13	2
SK	1	12	7	2	8	3	4	14	11	5	0	15	13	6	10	9
SK	10	7	6	1	0	14	3	13	12	9	11	2	15	5	4	8
SB	12	9	3	0	11	5	13	6	2	4	14	7	8	15	1	10
SB	3	8	14	1	5	2	11	13	10	4	9	7	6	15	12	0
SB	7	4	1	10	11	13	14	3	12	15	6	0	2	8	9	5
SB	6	3	1	4	10	12	15	2	5	14	11	8	9	7	0	13



<b>I<sub>5</sub></b>	<b>Kz5</b>	<b>Kz8</b>	<b>Kz11</b>	<b>Kz14</b>	<b>Kz17</b>	<b>Kz20</b>	<b>Kz23</b>	<b>Kz26</b>
<b>I<sub>6</sub></b>	<b>Kz6</b>	<b>Kz9</b>	<b>Kz12</b>	<b>Kz15</b>	<b>Kz18</b>	<b>Kz21</b>	<b>Kz24</b>	<b>Kz27</b>
<b>O<sub>0</sub></b>	<b>Kx0</b>	<b>Ky0</b>	<b>Ky1</b>	<b>Ky2</b>	<b>Ky3</b>	<b>Kx7</b>	<b>Kx8</b>	<b>Kx9</b>
<b>O<sub>1</sub></b>	<b>Kx1</b>	<b>Ky4</b>	<b>Ky5</b>	<b>Ky6</b>	<b>Ky7</b>	<b>Kx10</b>	<b>Kx11</b>	<b>Kx12</b>
<b>O<sub>2</sub></b>	<b>Kx2</b>	<b>Ky8</b>	<b>Ky9</b>	<b>Ky10</b>	<b>Ky11</b>	<b>Kx13</b>	<b>Kx14</b>	<b>Kx15</b>
<b>O<sub>3</sub></b>	<b>Kx3</b>	<b>Ky12</b>	<b>Ky13</b>	<b>Ky14</b>	<b>Ky15</b>	<b>Kx16</b>	<b>Kx17</b>	<b>Kx18</b>
<b>O<sub>4</sub></b>	<b>Kx4</b>	<b>Ky16</b>	<b>Ky17</b>	<b>Ky18</b>	<b>Ky19</b>	<b>Kx19</b>	<b>Kx20</b>	<b>Kx21</b>
<b>O<sub>5</sub></b>	<b>Kx5</b>	<b>Ky20</b>	<b>Ky21</b>	<b>Ky22</b>	<b>Ky23</b>	<b>Kx22</b>	<b>Kx23</b>	<b>Kx24</b>
<b>O<sub>6</sub></b>	<b>Kx6</b>	<b>Ky24</b>	<b>Ky25</b>	<b>Ky26</b>	<b>Ky27</b>	<b>Kx25</b>	<b>Kx26</b>	<b>Kx27</b>

Tables II & III – Diffusion networks for linear transformation unit 606/706

(continued in Table IV).

	<b>B1</b>	<b>B2</b>	<b>B3</b>	<b>B4</b>	<b>B5</b>	<b>B6</b>	<b>B7</b>	<b>B8</b>
<b>I<sub>0</sub></b>	<b>Bz0</b>	<b>By0</b>	<b>By4</b>	<b>By8</b>	<b>By12</b>	<b>By16</b>	<b>By20</b>	<b>By24</b>
<b>I<sub>1</sub></b>	<b>Bz1</b>	<b>By1</b>	<b>By5</b>	<b>By9</b>	<b>By13</b>	<b>By17</b>	<b>By21</b>	<b>By25</b>
<b>I<sub>2</sub></b>	<b>Bz2</b>	<b>By2</b>	<b>By6</b>	<b>By10</b>	<b>By14</b>	<b>By18</b>	<b>By22</b>	<b>By26</b>
<b>I<sub>3</sub></b>	<b>Bz3</b>	<b>By3</b>	<b>By7</b>	<b>By11</b>	<b>By15</b>	<b>By19</b>	<b>By23</b>	<b>By27</b>
<b>I<sub>4</sub></b>	<b>Bz4</b>	<b>Bz7</b>	<b>Bz10</b>	<b>Bz13</b>	<b>Bz16</b>	<b>Bz19</b>	<b>Bz22</b>	<b>Bz25</b>
<b>I<sub>5</sub></b>	<b>Bz5</b>	<b>Bz8</b>	<b>Bz11</b>	<b>Bz14</b>	<b>Bz17</b>	<b>Bz20</b>	<b>Bz23</b>	<b>Bz26</b>
<b>I<sub>6</sub></b>	<b>Bz6</b>	<b>Bz9</b>	<b>Bz12</b>	<b>Bz15</b>	<b>Bz18</b>	<b>Bz21</b>	<b>Bz24</b>	<b>Bz27</b>
<b>K<sub>0</sub></b>	<b>Ky0</b>	–	–	–	–	<b>Ky7</b>	<b>Ky14</b>	<b>Ky21</b>
<b>K<sub>1</sub></b>	<b>Ky1</b>	–	–	–	–	<b>Ky8</b>	<b>Ky15</b>	<b>Ky22</b>
<b>K<sub>2</sub></b>	<b>Ky2</b>	–	–	–	–	<b>Ky9</b>	<b>Ky16</b>	<b>Ky23</b>
<b>K<sub>3</sub></b>	<b>Ky3</b>	–	–	–	–	<b>Ky10</b>	<b>Ky17</b>	<b>Ky24</b>
<b>K<sub>4</sub></b>	<b>Ky4</b>	–	–	–	–	<b>Ky11</b>	<b>Ky18</b>	<b>Ky25</b>

combiner function 804, coupled to each other as shown. LFSRs 802 are collectively initialized with a stream cipher key, e.g. earlier described frame key  $K_i$ . During operation, the stream cipher key is successively shifted through LFSRs 802. Selective outputs are taken from LFSRs 802, and combiner function 804 is used to combine the selective outputs. In stream mode (under which, rekeying is enabled), the combined result is used to dynamically modify a then current state of a block cipher key in block key section 502.

For the illustrated embodiment, four LFSRs of different lengths are employed. Three sets of outputs are taken from the four LFSRs. The polynomials represented by the LFSR and the bit positions of the three sets of LFSR outputs are given by the table to follows:

LFSR	Polynomial	Combining Function		
		Taps		
		0	1	2
3	$X^{17} + X^{15} + X^{11} + X^5 + 1$	6	12	17
2	$X^{16} + X^{15} + X^{12} + X^8 + X^7 + X^5 + 1$	6	10	16
1	$X^{14} + X^{11} + X^{10} + X^7 + X^6 + X^4 + 1$	5	9	14
0	$X^{13} + X^{11} + X^9 + X^5 + 1$	4	8	13

Table V – Polynomials of the LFSR and tap positions.

The combined result is generated from the third set of LFSR outputs, using the first and second set of LFSR outputs as data and control inputs respectively to combiner function 802. The third set of LFSR outputs are combined into a single bit. In stream mode (under which, rekeying is enabled),

Referring now to back to **Figure 5**, as illustrated and described earlier, mapping function **508** generates the pseudo random bit sequence based on the contents of selected registers of block key section **502** and data section **504**. In one embodiment, where block key section **502** and data section **504** are implemented in accordance with the respective embodiments illustrated in **Fig. 6-7**, mapping function **508** generates the pseudo random bit sequence at 24-bit per clock based on the contents of registers (Ky and Kz) **602b-602c** and (By and Bz) **702b-702c**. More specifically, each of the 24 bits is generated by performing the XOR operation on nine terms in accordance with the following formula:

$$(B0 \cdot K0) \oplus (B1 \cdot K1) \oplus (B2 \cdot K2) \oplus (B3 \cdot K3) \oplus (B4 \cdot K4) \oplus (B5 \cdot K5) \oplus (B6 \cdot K6) \oplus B7 \oplus K7$$

Where " $\oplus$ " represents a logical XOR function, " $\cdot$ " represents a logical AND function, and the input values B and K for the 24 output bits are

Input Origin Output bit	B0 Bz	B1 Bz	B2 Bz	B3 Bz	B4 Bz	B5 Bz	B6 Bz	B7 By	K0 Kz	K1 Kz	K2 Kz	K3 Kz	K4 Kz	K5 Kz	K6 Kz	K7 Ky
	14	23	7	27	3	18	8	20	12	24	0	9	16	7	20	13
	20	26	6	15	8	19	0	10	26	18	1	11	6	20	12	19
	7	20	2	10	19	14	26	17	1	22	8	13	7	16	25	3
	22	12	6	17	3	10	27	4	24	2	9	5	14	18	21	15
	22	24	14	18	7	1	9	21	19	24	20	8	13	6	3	5
	12	1	16	5	10	24	20	14	27	2	8	16	15	22	4	21
	5	3	27	8	17	15	21	12	14	23	16	10	27	1	7	17
	9	20	1	16	5	25	12	6	9	13	22	17	1	24	5	11
	23	25	11	13	17	1	6	22	25	21	18	15	6	11	1	10
	4	0	22	17	25	10	15	18	0	20	26	19	4	15	9	27
1	23	25	9	2	13	16	4	8	2	11	27	19	14	22	4	7
1	3	6	20	12	25	19	10	27	24	3	14	6	23	17	10	1
1	26	1	18	21	14	4	10	0	17	7	26	0	23	11	14	8
1	2	11	4	21	15	24	18	9	5	16	12	2	26	23	11	6
1	22	24	3	19	11	4	13	5	22	0	18	8	25	5	15	2
1	12	0	27	11	22	5	16	1	10	3	15	19	21	27	6	18

CLAIMS

What is claimed is:

1. In a video source device, a method comprising:  
generating a session key for a transmission session within which a multi-frame video content is to be transmitted to a video sink device; and  
generating a successive number of frame keys, using at least the session key, to facilitate ciphering of corresponding frames of the multi-frame video content for transmission to the video sink device.
2. The method of claim 1, wherein said generating of successive frame keys comprises generating at each vertical blanking interval of said multi-frame video content, a frame key for ciphering a frame of said multi-frame video content.
3. The method of claim 2, wherein said method further comprises generating a pseudo random bit sequence for each frame, using at least the corresponding frame key, for ciphering the particular frame of said multi-frame video content.
4. The method of claim 3, wherein each of said generating of a pseudo random bit sequence using a corresponding frame key comprises successive modifications of the corresponding frame key.
5. The method of claim 4, wherein said successive modifications of the corresponding frame key are performed at horizontal blanking intervals of the frame.
6. The method of claim 3, wherein said method further comprises generating an initial pseudo random bit sequence using at least the session key, and deriving an initial pseudo random number from the initial pseudo random bit sequence to be used with a first frame key to generate a first pseudo random bit sequence to cipher a first frame.
7. The method of claim 3, wherein each of said generating of a pseudo random bit sequence comprises generating sufficient number of pseudo random bits for ciphering a pixel on a bit-wise basis each clock.
8. In a video source device, a method comprising:  
generating a frame key for each frame of a multi-frame video content; and  
generating a pseudo random bit sequence for each of the corresponding frames, using at least the corresponding frame key, for ciphering the video content.
9. The method of claim 8, wherein said generating of a frame key for each frame comprises generating one frame key at each vertical blanking interval of said multi-frame video content.

17. The apparatus of claim 13, wherein the block cipher comprises a first and a second register to store a first and a second value, and a function block coupled to the first and second registers to transform the stored first and second values, with a selected one of the transformed first and second values being the session key or a frame key.
18. The apparatus of claim 17, wherein the block cipher is an integral part of said stream cipher.
19. In a video sink device, a method comprising:  
generating a session key for a reception session within which a multi-frame video content is to be received from a video source device; and  
generating a successive number of frame keys, using at least the session key, to facilitate deciphering of corresponding frames of the multi-frame video content received from the video source device.
20. The method of claim 19, wherein said generating of successive frame keys comprises generating at each vertical blanking interval of said multi-frame video content, a frame key for deciphering a frame of said multi-frame video content.
21. The method of claim 20, wherein said method further comprises generating a pseudo random bit sequence for each frame, using at least the corresponding frame key, for deciphering the particular frame of said multi-frame video content.
22. The method of claim 21, wherein each of said generating of a pseudo random bit sequence using a corresponding frame key comprises successive modifications of the frame key.
23. The method of claim 22, wherein said successive modifications are performed at horizontal blanking intervals of the frame.
24. The method of claim 21, wherein said method further comprises generating an initial pseudo random bit sequence using at least the session key, and deriving an initial pseudo random number from the initial pseudo random bit sequence to be used with the first frame key to generate a first pseudo random bit sequence to cipher a first frame.
25. The method of claim 21, wherein each of said generating of a pseudo random bit sequence comprises generating sufficient number of pseudo random bits for deciphering a pixel on a bit-wise basis each clock.
26. In a video sink device, a method comprising:  
generating a frame key for each frame of a multi-frame video content received from a video source device; and

1/5

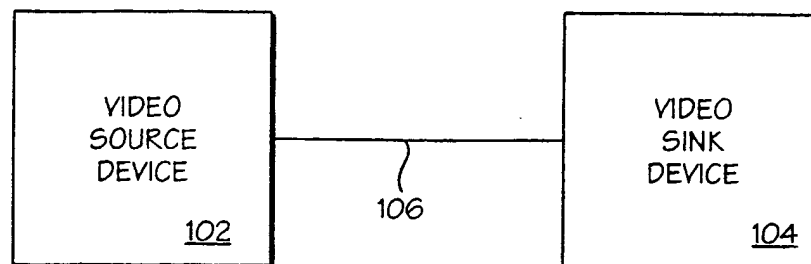


FIG. 1

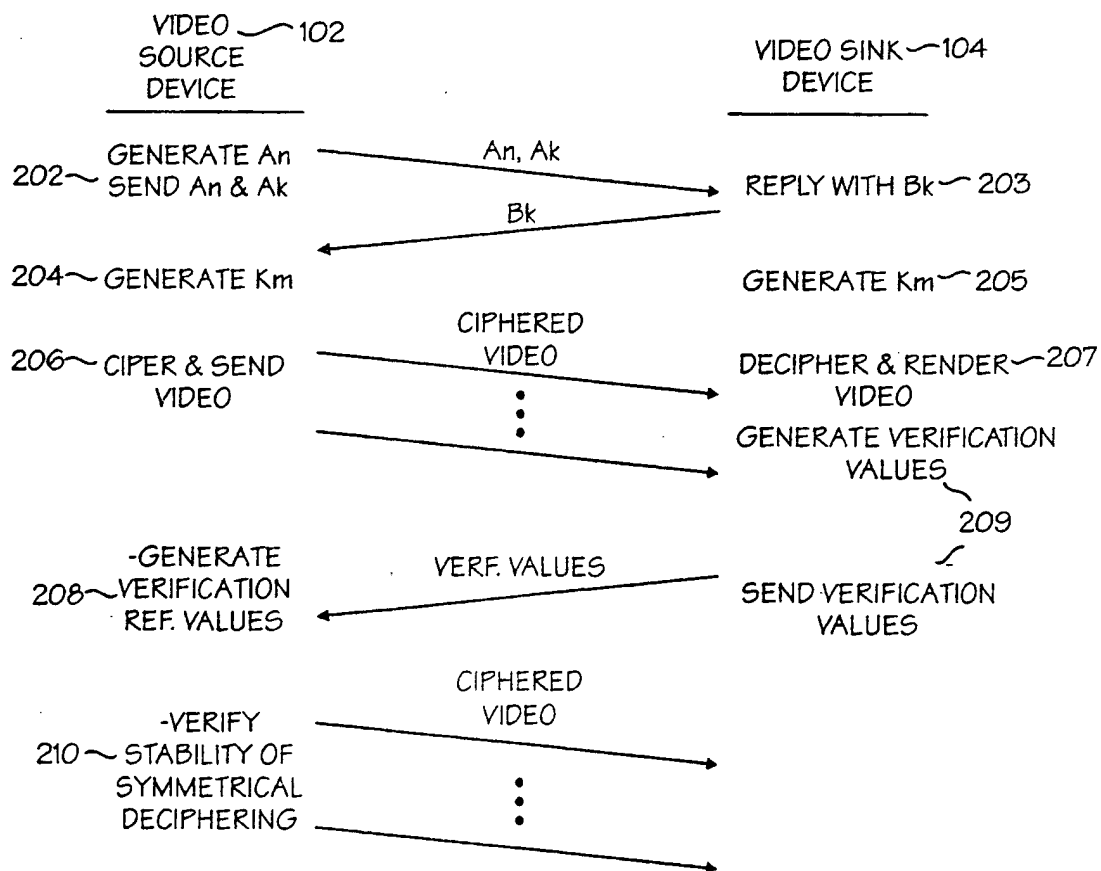


FIG. 2

2/5

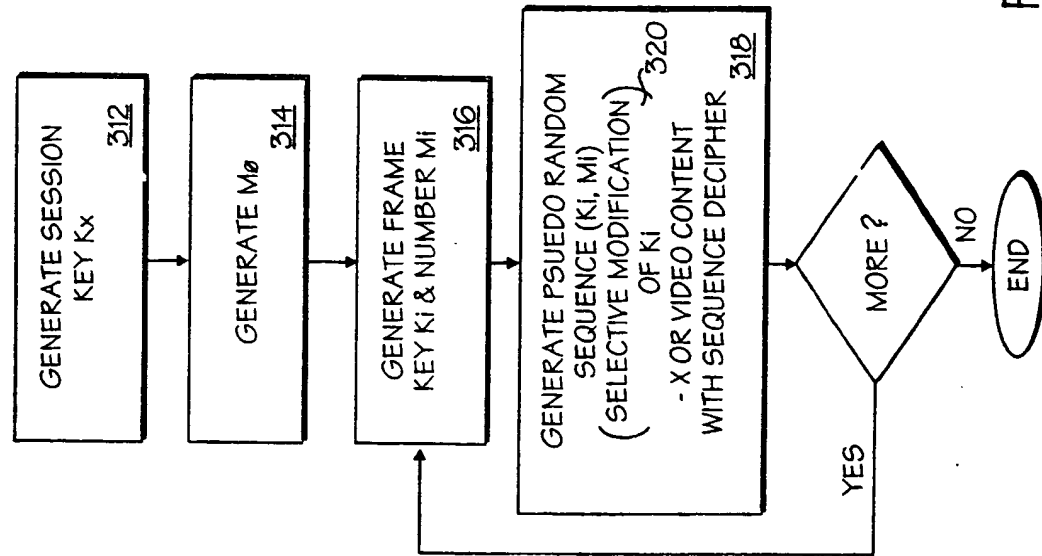


Fig. 3a

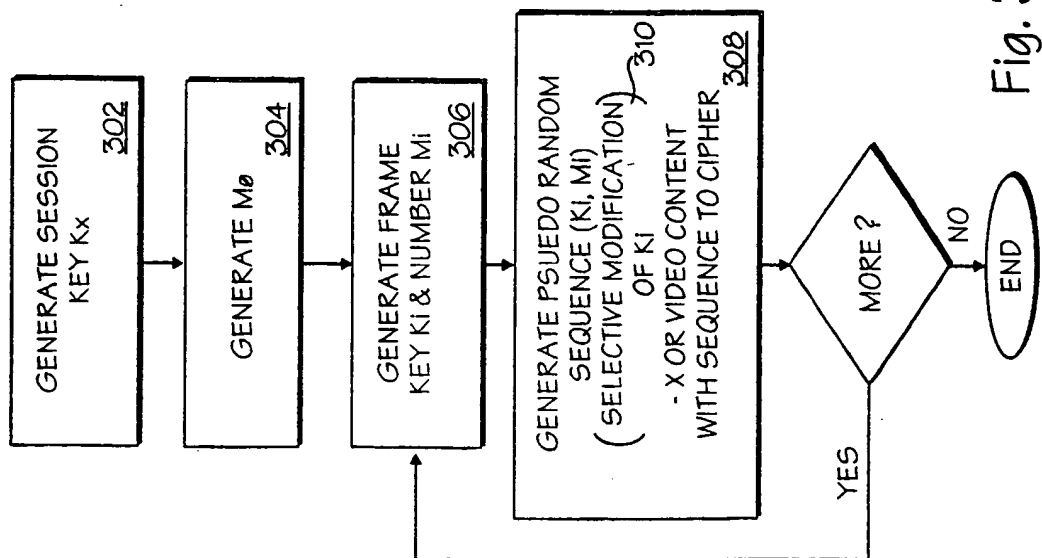


Fig. 3b

3/5

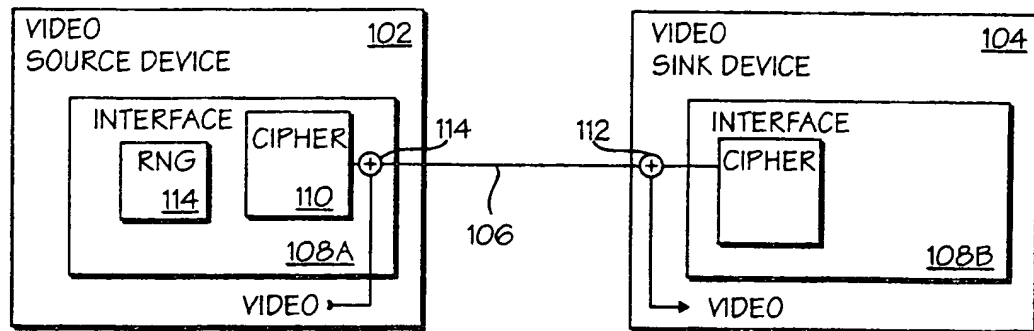


FIG. 4

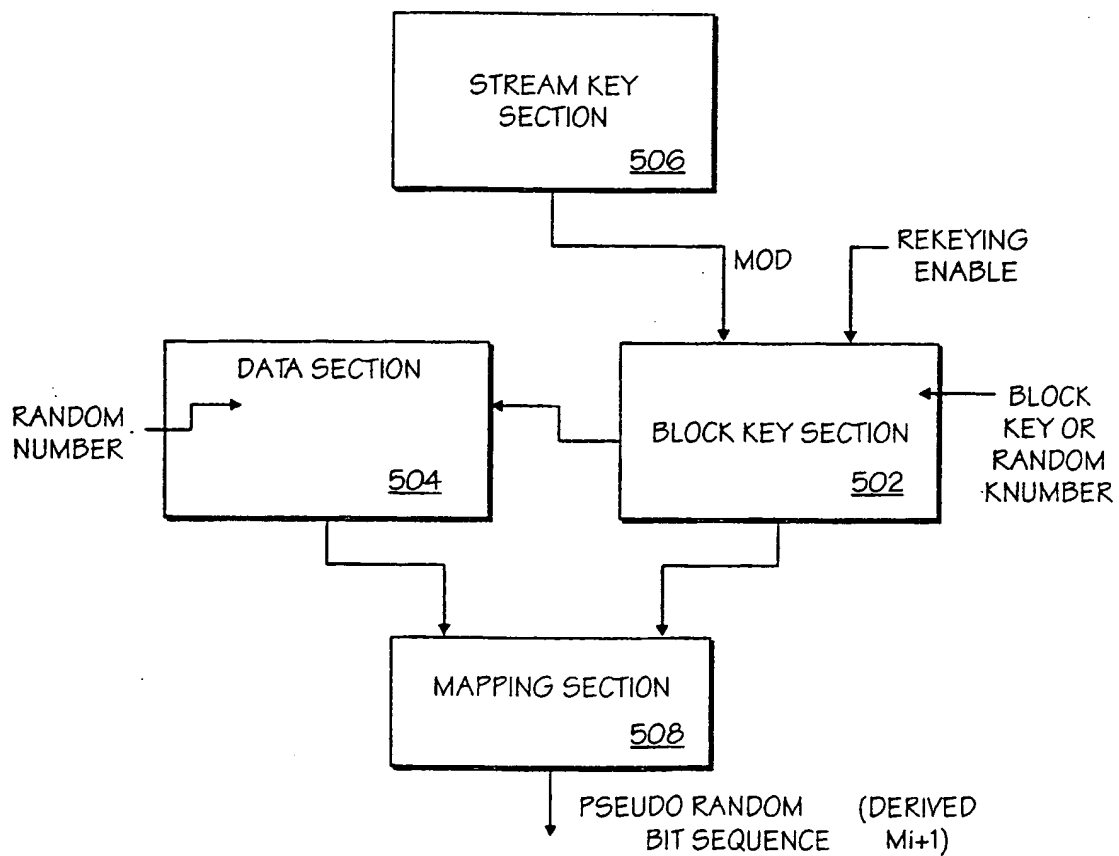


FIG. 5



4/5

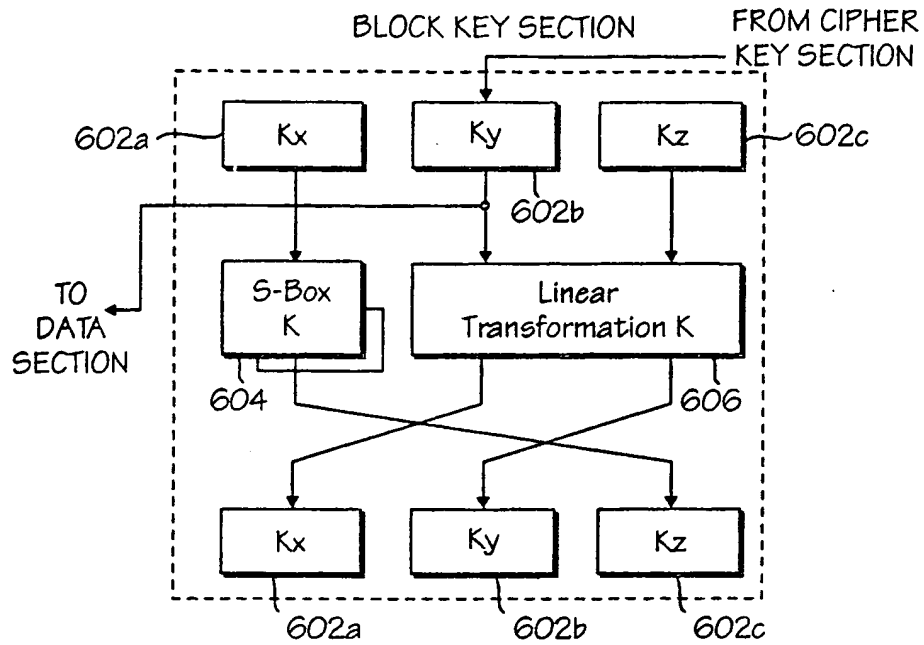


FIG. 6

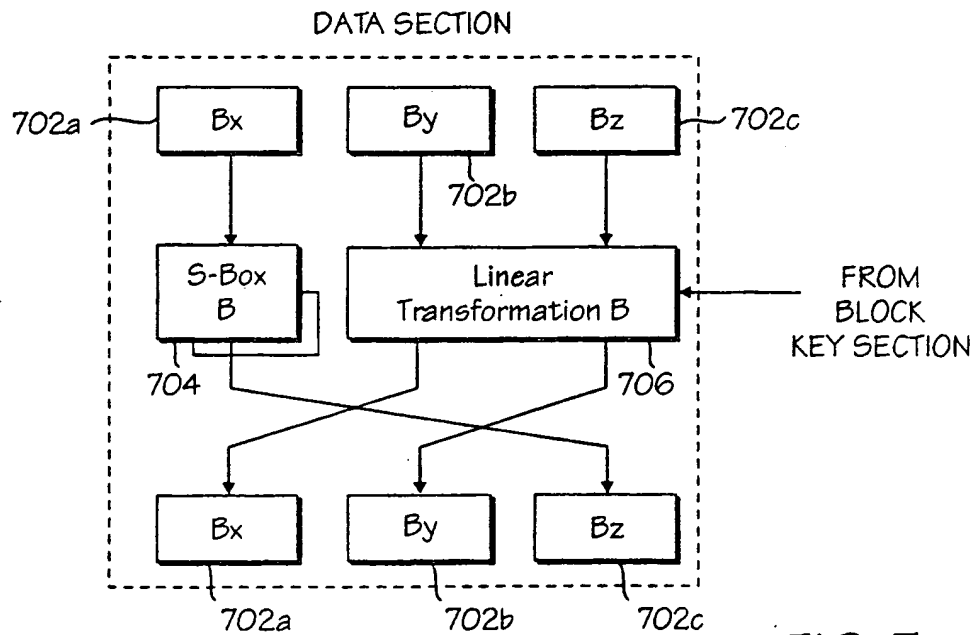
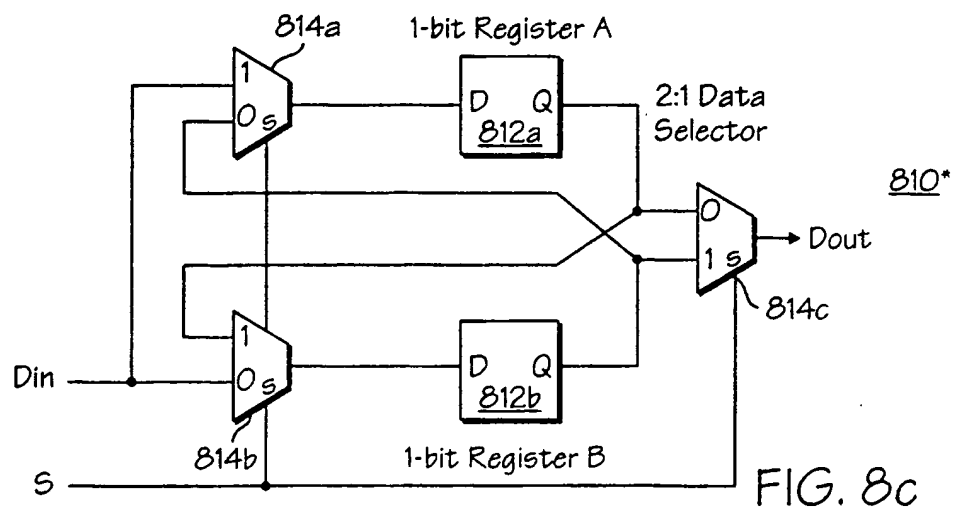
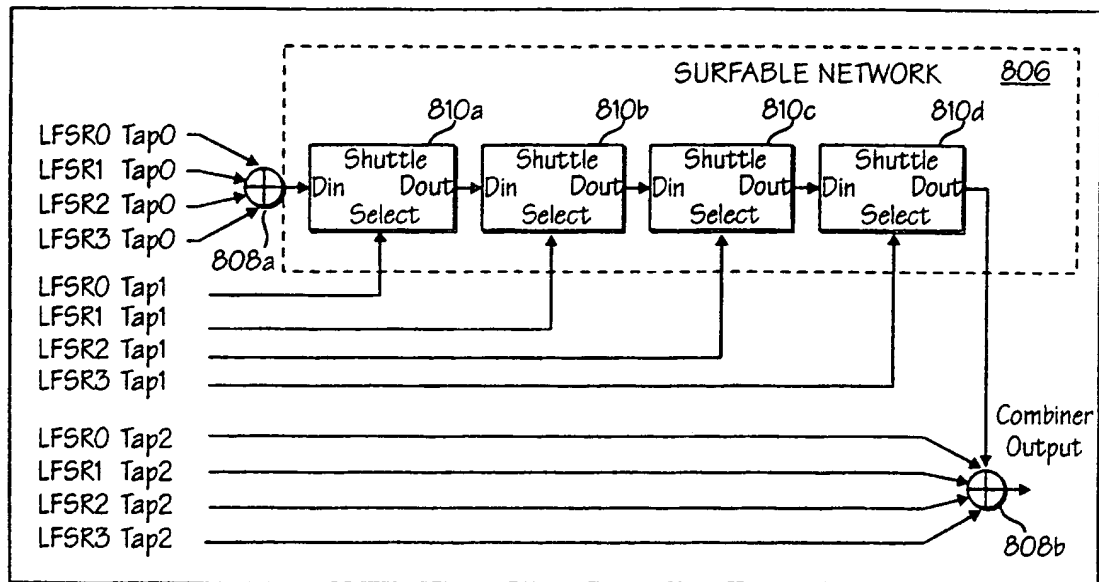
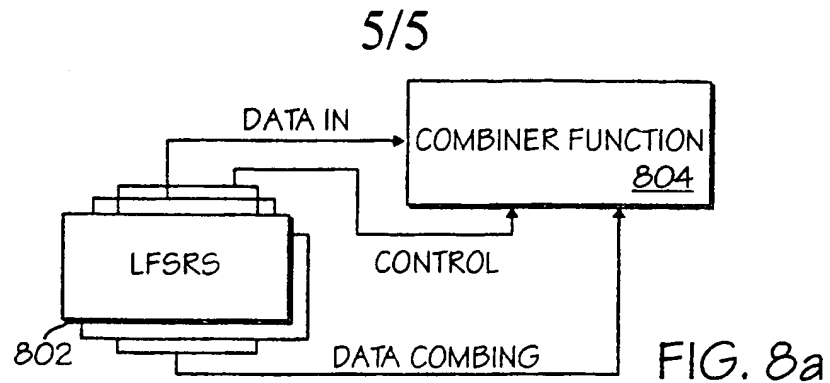


FIG. 7



# INTERNATIONAL SEARCH REPORT

International Application No

PCT/US 00/22785

<b>A. CLASSIFICATION OF SUBJECT MATTER</b> IPC 7 H04N7/167		
According to International Patent Classification (IPC) or to both national classification and IPC		
<b>B. FIELDS SEARCHED</b>		
Minimum documentation searched (classification system followed by classification symbols) IPC 7 H04N		
Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched		
Electronic data base consulted during the international search (name of data base and, where practical, search terms used) EPO-Internal		
<b>C. DOCUMENTS CONSIDERED TO BE RELEVANT</b>		
Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	WO 99 18729 A (BENARDEAU CHRISTIAN ; CANAL PLUS SA (FR); MAILLARD MICHEL (FR); DAU) 15 April 1999 (1999-04-15) page 7, line 27 - line 30 page 8, line 24 - page 12, line 16 figures 3-5	1-36
A	US 5 621 799 A (IBARAKI SUSUMU ET AL) 15 April 1997 (1997-04-15) column 3, line 3 - column 8, line 19 figures 1-4	1-36
A	US 5 852 472 A (GUTMANN MICHAEL J ET AL) 22 December 1998 (1998-12-22) column 1, line 14-29 figure 3	1,13,19, 26,30,31
-/--		
<div style="display: flex; justify-content: space-between;"> <span><input checked="" type="checkbox"/> Further documents are listed in the continuation of box C.</span> <span><input checked="" type="checkbox"/> Patent family members are listed in annex.</span> </div>		
<div style="display: flex;"> <div style="flex: 1;"> <p>* Special categories of cited documents:</p> <p>*A* document defining the general state of the art which is not considered to be of particular relevance</p> <p>*E* earlier document but published on or after the international filing date</p> <p>*L* document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)</p> <p>*O* document referring to an oral disclosure, use, exhibition or other means</p> <p>*P* document published prior to the international filing date but later than the priority date claimed</p> </div> <div style="flex: 1;"> <p>*T* later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention</p> <p>*X* document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone</p> <p>*Y* document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.</p> <p>*Z* document member of the same patent family</p> </div> </div>		
Date of the actual completion of the international search <div style="text-align: center; font-weight: bold;">29 November 2000</div>		Date of mailing of the international search report <div style="text-align: center; font-weight: bold;">06/12/2000</div>
Name and mailing address of the ISA European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040. Tx. 31 651 epo nl. Fax: (+31-70) 340-3016		Authorized officer <div style="text-align: center; font-weight: bold; font-size: 1.2em;">Van der Zaal, R</div>

# INTERNATIONAL SEARCH REPORT

Information on patent family members

International Application No

PCT/US 00/22785

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
WO 9918729 A	15-04-1999	AU 9278298 A BR 9812703 A EP 1020080 A NO 20001649 A ZA 9808951 A	27-04-1999 22-08-2000 19-07-2000 02-06-2000 12-04-1999
US 5621799 A	15-04-1997	JP 7115414 A JP 7134647 A	02-05-1995 23-05-1995
US 5852472 A	22-12-1998	NONE	
US 4953208 A	28-08-1990	JP 2288573 A JP 2810103 B GB 2232032 A,B	28-11-1990 15-10-1998 28-11-1990

**This Page is Inserted by IFW Indexing and Scanning  
Operations and is not part of the Official Record**

## **BEST AVAILABLE IMAGES**

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images include but are not limited to the items checked:

- ☐ **BLACK BORDERS**
- ☐ **IMAGE CUT OFF AT TOP, BOTTOM OR SIDES**
- ☐ **FADED TEXT OR DRAWING**
- ☒ **BLURRED OR ILLEGIBLE TEXT OR DRAWING**
- ☐ **SKEWED/SLANTED IMAGES**
- ☐ **COLOR OR BLACK AND WHITE PHOTOGRAPHS**
- ☐ **GRAY SCALE DOCUMENTS**
- ☐ **LINES OR MARKS ON ORIGINAL DOCUMENT**
- ☐ **REFERENCE(S) OR EXHIBIT(S) SUBMITTED ARE POOR QUALITY**
- ☐ **OTHER: \_\_\_\_\_**

### **IMAGES ARE BEST AVAILABLE COPY.**

**As rescanning these documents will not correct the image problems checked, please do not report these problems to the IFW Image Problem Mailbox.**